DOI: http://doi.org/10.25728/cs.2022.1.6

29TH INTERNATIONAL CONFERENCE ON PROBLEMS OF COMPLEX SYSTEMS SECURITY CONTROL

In December 2020, the 29th International Conference on Problems of Complex Systems Security Control took place at Trapeznikov Institute of Control Sciences, Russian Academy of Sciences (RAS), Moscow. The conference was organized by the Ministry of Science and Higher Education of the Russian Federation, Trapeznikov Institute of Control Sciences RAS, Keldysh Institute of Applied Mathematics RAS, the RAS Scientific Council on the Theory of Controlled Processes and Automation, and the Ministry of the Russian Federation for Civil Defense, Emergencies and Elimination of Consequences of Natural Disasters.

The conference was attended by 123 authors from 49 organizations (Russia and several foreign countries). The conference program included 84 papers in eight sections:

1. Theoretical and methodological questions of security support;
2. Problems of economic and sociopolitical security support;
3. Problems of information security support;
4. Cybersecurity. Security aspects in social networks;
5. Ecological and technogenic security;
6. Modeling and decision-making for complex systems security control;
7. Automatic systems and means of complex systems security support;
8. Legal aspects of complex systems security support.

This annual conference traditionally takes place in the second half of December. The past 2021 was extremely tense and eventful. First of all, note the growing complexity of counteraction to the COVID-19 pandemic due to the emergence of new virus mutations. Despite the need to consolidate the efforts of the global community for the survival of humanity in the face of the pandemic, the international situation continued to deteriorate, and the crisis in relations between Russia and Western countries deepened, taking the form of intense military-political and economic confrontation, as well as an open information war.

The COVID-19 pandemic and the resulting global financial crisis affected foreign economic relations, world trade, and the domestic commodity and financial markets of even relatively prosperous countries. These negative processes resulted in large-scale bankruptcies of small businesses, job cuts, employment problems, and the need to transfer employees of many organizations to the remote working mode, causing a significant increase in cybercrimes using remote attacks, phishing, social engineering technologies, etc. In addition, new types of cybercrimes emerged, including those exploiting the COVID-19 topic in various ways.

The year 2021 will also be remembered for natural and climatic anomalies: abnormal heat in Russia, the USA, Canada, and several European countries; large-scale forest fires in Yakutia (Russia), Turkey, Greece, and the USA; floods in the Crimea and Krasnodar Krai (Russia), the Far East, China, India, Austria, Czech Republic, Germany, and other countries; typhoons and downpours in the Far East; an unprecedentedly destructive tornado in the USA; frosts in Africa and South America, etc. There is still no consensus in the scientific community about their causes. Also, there were man-induced accidents and disasters at industrial and transport facilities.

The current situation and explicit negative trends of further development (possible or even quite probable in some areas) call for comprehensive measures and systemic mechanisms to improve the effectiveness of countering various external and internal threats to the security of individuals, society, and the state. These factors increase the relevance and importance of comprehensive interdisciplinary (fundamental and applied) research of methods, tools, and mechanisms to improve the effectiveness of security control (in the broadest sense). No doubt, it affected the topics of conference papers.

According to an established tradition, the conference was opened with a detailed paper, “How not to be in the sixteenth century,” by *G.G. Malinetskii, V.V. Kul’ba, T.S. Akhromeeva, S.A. Toropygina, and S.A. Posashkov*. The authors analyzed the impact of the ongoing global changes and growing contradictions in world development and the associated risks and threats. The paper considered key strategic objectives for developing Russian society and the state in the long term. Much attention was paid to the problems in culture, science, high technologies, and demography aggravated by the pandemic and other priority tasks of progressive economic development of the country. Based on the analysis of risks and global threats to the Russian state and society, the authors focused on the ways out of the current difficult situation to achieve the basic national development goals of the Russian Federation in the short and long run.

For the second year, conference participants dealt with improving the efficiency of counteraction to the COVID-19 pandemic in their papers. Among them, note the paper "A technology to create monitoring and forecasting systems for the state of dangerous phenomena and objects (on the example of COVID-19 pandemic)" by *A.V. Sokolov, G.V. Roizenzon, and N.P. Komendantova*. It was devoted to developing a methodology to assess the effectiveness of restrictive measures as a tool to combat the spread of COVID-19. Three basic groups of effectiveness criteria were identified: available resources of different types (bedspace, medical staff, equipment, medicines, etc.); the rates of spending and replenishing necessary resources to combat the pandemic; the degree of achieving the set goals. To assess the effectiveness of restrictive measures, the authors proposed applying multicriteria order classification and verbal analysis methods for decisions made. Also, the paper generalized the experience accumulated by the authors in monitoring and forecasting new COVID-19 cases in Moscow in 2020 and 2021.

The problems of counteraction to the pandemic were also addressed in the following papers: "On a peculiarity of modeling the first stage of COVID-19 infection" by *M.E. Stepantsov*; "New models of SARS-CoV-2 virus spread and security control problems" by *N.G. Kereselidze*; "The impact of COVID-19 restrictions on economic systems security" by *T.Kh. Usmanova and N.N. Volodina*.

A distinctive feature of the conference is numerous papers on various topics, presenting research results on a wide range of methodological and applied problems of improving the effectiveness of security control processes in the context of digitalization, the rapid development of information and communication technologies, and the threats and risks associated with these processes.

A research group headed by *V.L. Shultz*, Corresponding Member of the RAS, presented the paper "Analysis of the uncertainty factor in preparing managerial decisions." The authors considered the problems of increasing the efficiency of organizational management under risk. As stated in the paper, such uncertainty has two main sources: the subjective (epistemological) source due to insufficient knowledge necessary for making managerial decisions, and the objective (aleatoric, ontological) source due to the stochastic nature of the control object or its environment. A separate class is a linguistic (subjective) uncertainty due to several objective properties of natural language. According to the authors, the methodology for evaluating uncertainty factors is being developed mainly towards methods for applied problems within the studied segments of subject areas due to the multifaceted character of uncertainty. Attempts to develop universal methods for assessing the impact of uncertainty on the effectiveness of managerial decisions face significant difficulties. They can be partially overcome using scenario analysis.

In the paper "Cryptocurrencies as a threat to the national security of Russia: legal counteraction mechanisms," *A.A. Timoshenko* considered problems caused by the lack of legal regulation of many aspects of cryptocurrency circulation in the Russian Federation. With the worldwide recognition of cryptocurrencies as an instrument of forming alternative financial relations, the author paid special attention to the analysis of threats to the national security of Russia, particularly in the situation when virtual currencies are used for illegal purposes. Threats to uncontrolled circulation of cryptocurrencies were analyzed in terms of goals, objectives, and functions of law enforcement agencies. As a result, detailed proposals to improve the Russian system of legislative regulation were formulated, including the introduction of appropriate changes in the current legislation and vesting the Government and relevant agencies with the power to regulate and control the circulation of digital financial assets. Fully agreeing with the conclusions of the author, we emphasize the growing relevance of the problems considered in the paper: the mass use of cryptocurrencies in the national payment cycle and numerous issuers uncontrolled by the state may eventually lead to a critical disorder of the financial system and, most importantly, to the inability to effectively plan and implement a uniform monetary policy of the state with all the ensuing negative consequences.

Traditionally, conference participants are interested in the problems of information and cybersecurity control. *R.V. Meshcheryakov* presented the paper "An approach to secure intelligent control of robots and their coalitions using human-robot(s) and robot-robot(s) interfaces." He considered the problems of forming secure mechanisms of inter-machine data exchange. The topicality of such research is currently increasing due to the development of the Internet of Things and the absence of security standards for robotic control systems using human-machine interfaces. As shown in the paper, the developed models and security mechanisms of the systems should be based on different interfaces for redundant communication channels when giving commands and receiving feedback from control objects. In addition, these models and mechanisms should consider such factors as noise immunity of measuring channels, fault tolerance of the entire system, the reproducibility of the reference signal, and the presence of a single transmission format for measurement information.

This broad topic was also treated in the following papers: “A two-factor authentication algorithm as a tool to reduce FRR for a proactive attack detection filter” by *A.M. Smirnov and A.Yu. Iskhakov*; “Situational awareness for the safe and effective operation of agrorobots” by *V.K. Abrosimov and A.N. Raikov*; “Some issues in the verification and validation process of cybersecurity control” by *E.F. Jharko*; “A concept of information security for a swarm of cyber-physical systems” by *D.I. Pravikov*; “Determining the success of intruder’s actions in a homogeneous environment” by *K.A. Bugaiskii*; “Using SSL/TLS technology to create secure network channels in distributed systems” by *R.E. Asratyan*; “Methods to counteract tracing user’s browser fingerprints” by *A.A. Salomatina*; “Service-browser and Man-in-the-middle attacks” by *V.L. Orlov and E.A. Kurako*; “The problem of optimizing the reconstruction scheme of destroyed operating data reserve in distributed systems” by *S.K. Somov*; “Information reliability as an element of information security and assessment of its level” by *A.D. Kozlov and N.L. Noga*; “Goals, tasks, and principles of security of digital intellectual property management systems” by *V.O. Sirotyuk*; “Ensuring the continuous development of software products certified by security requirements” by *A.A. Melikhov*.

Several interesting papers were devoted to topical security problems in social networks. Among them, we mention the following: “Features of mathematical tools used to build security systems in social networks” by *L.V. Zhukovskaya*; “Systematization of psychological factors to change beliefs and attitudes as a result of communicative influences in the form of causal influence model” by *Z.K. Avdeeva and S.V. Kovriga*; “Assessment of risks of destructive content in social networks” by *M.V. Mamchenko and A.S. Rey*; “Ethical aspects of applying artificial intelligence tools to ensure the space of trust in electronic media” by *G.K. Boreskov*; “Developing a dynamic system for the operation of social network communities” by *E.P. Okhapkina*; “Digitalization: threats and risks” by *V.V. Muromtsev and A.V. Muromtseva.*

Conference participants presented many interesting papers on problems of managing economic, environmental, energy, and technogenic security in the context of high-tech development, associated recently with the international “green” or “climate” agenda. However, the declared and real goals of this agenda are a separate subject of detailed analysis widely discussed by scientific and expert communities.

In the paper “Safety of the aquatic ecosystem of Azov–Black Sea region: cognitive study,” *G.V. Gorelova, E.V. Melnik, M.V. Orda-Zhigulina, and D.V. Orda-Zhigulina* performed the cognitive analysis and simulation of processes in the regional aquatic ecosystem to predict environmental threats and ensure the safety of the population and coastal infrastructure. The authors presented the functional structure of an original monitoring system for hazardous phenomena in natural systems, designed to observe the corresponding processes continuously.

The approach proposed by the authors is promising: a single monitoring system integrates diverse and multi-temporal data from various sources to reveal (particularly implicit) cause-effect relations between the parameters of the hydro-ecosystem studied by traditional methods. Thus, the system determines the patterns of ecosystem processes and provides intellectual support for decision-making processes to counteract environmental threats based on cognitive modeling.

Among the contributions on this broad topic, note the following papers: “Problems of managing the development of large-scale socio-economic systems” by *N.N. Volodina, N.I. Komkov, and V.V. Sutyagin*; “Formalization of institutions, adverse selection, and control of agents’ corrupt behavior” by *R.M. Nizhegorodtsev*; “Preparation of Russian public administration system for supercritical situations of natural and man-induced character” by *E.P. Grabchak and E.L. Loginov*; “On an approach to critical infrastructure risk management” by *E.A. Abdulova*; “Structural stability of the Arctic as a territorial economic ecosystem” by *N.N. Lanter*; “Digital transformation and import substitution related to nuclear facility security” by *T.A. Piskureva and A.N. Makhov*; “A system approach to the application of artificial intelligence to resolve environmental safety problems in the digital transformation of agriculture” by *V.I. Medennikov*; “Fundamentals of information support of electricity supply under the destructive impact of hydrometeorological factors” by *M.A. Polyukhovich*; “Integrated geo-ecological monitoring of forest geo-ecosystems of the Moscow metropolitan region” by *R.E. Torgashev.*

Traditionally, conference participants show great interest in the problems of technogenic and industrial security. In the paper “Management of cybersecurity risk at the design stage of industrial systems,” *V.G. Promyslov and K.V. Semenkov* described a cybersecurity risk assessment technology for the design process of critical industrial facilities. The proposed technology consists of two basic stages. The first stage includes a general risk assessment for the system to be designed under uncertainty in understanding the details of system implementation and, in part, the requirements imposed on it. In this stage, the basic technical solutions for cybersecurity are laid down. Moreover, the generalized assessments of risks can be used to prioritize their detailed elaboration when designing the security architecture of critical industrial facilities (e.g., for division into security zones or classification of assets). The second (optional) stage includes a detailed risk assessment considering the specifics of the system architecture and the threat model.

The proposed technology has several advantages: the ability to prevent critical errors in the system design process due to the under- or overestimation of cybersecurity requirements; the ability to reduce the volume (the cost and time) of design work by eliminating detailed risk assessment procedures for individual subsystems if the integral assessment for the entire system does not exceed a given threshold.

Several interesting papers were devoted to the problems of prevention and elimination of man-induced and natural emergencies and the safety and reliability of technological complexes and transport systems: "Increasing the safety of managing complex objects under implicit variations of technological process parameters" by *V.O. Chinakal*; "Safe dispatch control in intelligent unmanned traffic control systems" by *L.A. Baranov, E.P. Balakina, and V.G. Sidorenko;* "Mathematical modeling of seismic stress waves in a half-plane by a vertical cavity of rubber: a width-to-height ration of 1:10" by *V.K. Musaev*; "Stochastic modeling of cascade scenarios of accidents and disasters" by *M.Yu. Prus*; "Fire security analysis of a thermal power plant based on the study of fire hazards" by *A.V. Evdokimova*; "On the justification of industrial safety audit" by *E.V. Klovach and V.A. Tkachenko*; "Vibration fatigue of mechanisms and machines: standardization and rate setting" by *O.B. Skvortsov*.

In addition, note several conference papers of different topics united by the topicality of the problems considered and the demand for their solutions: "Tools for digitalizing the personnel security management of a regional production cluster" by *V.V. Bystrov, A.V. Masloboev, and I.O. Datiev*; "Natural computing in risk management of complex systems: models and methods" by *A.A. Shiroky*; "Risk management of a complex computer network based on a general arbitration scheme" by *E. V. Anikina*; "Fundamentals of modeling information security measures to ensure the conflict stability of socio-economic organizations" by *L.E. Mistrov and E. Golovchenko*; "A methodology for calculating economic damage from drug addiction" by *A.N. Fomichev*; "Migration policy and city security" by *V.V. Kafidov*; "National security in the sphere of intellectual property in Russia" by *V.V. Leshchenko*; "Information decision support means for assessing the capabilities of technical intelligence" by *I.A. Sidorenko, O.N. Dudarikov, and N.E. Khodyreva*; "Analysis of applied ways to increase the metrological reliability of measuring transducers" by *A.M. Anokhin*; "Peculiarities of estimating vibration influences in electromechanical systems with pulse control" by *V.I. Stashenko, O.B. Skvortsov, and O.A. Troitsky*; "Computational load balancing under the parallel solution of a minimax scheduling problem by the branch-and-bound method" by *D.R. Gonchar.*

The papers can be found in the conference proceedings[1] or on the official conference website: URL:https://iccss2021.ipu.ru/prcdngs.

In his closing remarks, the Conference Chair, Dr. Sci. (Eng.), Prof. *V.V. Kul'ba* announced plans to hold the 30th Anniversary International Conference on Problems of Complex Systems Security Control, according to the established tradition, in December 2022 at Trapeznikov Institute of Control Sciences RAS. Please contact the Organizing Committee via phone + 7 495 198-17-20 (ext. 1407) or e-mail iccss@ipu.ru. The Technical Secretary of the conference is *Alla Farissovna Ibragimova*.

Academic Secretary of the Organizing Committee
A.B. Shelkov

Author information
Shelkov, Alexey Borisovich. Cand. Sci. (Eng.), Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia
✉ abshelkov@gmail.com

Cite this paper
Shelkov, A.B. 29th International Conference on Complex Systems Security Control. *Control Sciences* **1**, 61–64 (2022). http://doi.org/10.25728/cs.2022.1.6

Original Russian Text © Shelkov, A.B., 2022, published in *Problemy Upravleniya*, 2022, no. 1, pp. 75–80.

Translated into English by *Alexander Yu. Mazurov,*
Cand. Sci. (Phys.-Math.),
Trapeznikov Institute of Control Sciences,
Russian Academy of Sciences, Moscow, Russia
✉ alexander.mazurov08@gmail.com

[1] Materialy 29-oi Mezhdunarodnoi konferentsii "Problemy upravleniya bezopasnost'yu slozhnykh sistem" (Proceedings of 29th International Conference on Complex Systems Security Control), December 15, 2021, Moscow, Kalashnikov, A.O. and Kul'ba, V.V., Eds., Moscow: Trapeznikov Institute of Control Sciences RAS, 2021. (In Russian.)